

[print](#) | [export](#)

Publication number: JP2002216275 A2
Publication country: JAPAN
Publication type: APPLICATION
Publication date: 20020802
Application number: JP20010005651
Application date: 20010112
Priority: JP20010005651 20010112 ;
Assignee: SOGO KEIBI HOSHO CO LTD ;
Assignee^{std}: SOGO KEIBI HOSHO KK ;
Inventor^{std}: OGAWA UHITO ;
International class¹⁻⁷: G08B25/10 ; H04N7/16 ; H04N7/173 ; H04N7/18 ;
International class⁸: H04N7/18 20060101 I C ; H04N7/18 20060101 I A ; G08B25/10 20060101 I C ; G08B25/10 20060101 I A ; H04N7/16 20060101 I C ; H04N7/16 20060101 I A ; H04N7/17 20060101 I C ; H04N7/17 20060101 I A ;
Title: MONITORING SYSTEM
Abstract: PROBLEM TO BE SOLVED: To provide a monitoring system protecting the privacy more strongly when confirming an image in a monitoring area by accessing an image server. SOLUTION: In password authentication or an URL input when a portable terminal 200 is confirming the image of a monitoring object 100 by accessing the image server 400, a monitoring management device 300 updates an image page of a predetermined address managed by the image server 400 to an image page of an up-to-date image of the monitoring object 100, it issues a password necessary for a user authentication for accessing the image page or a URL necessary when specifying the image page, and it sends it to the portable terminal 200.

(51) Int.Cl. ⁷	識別記号	F I	キーワード (参考)
G 0 8 B 25/10		G 0 8 B 25/10	D 5 C 0 5 4
H 0 4 N 7/16		H 0 4 N 7/16	Z 5 C 0 6 4
7/173	6 3 0	7/173	6 3 0 5 C 0 8 7
7/18		7/18	D
			U

審査請求 未請求 請求項の数 6 ○ L (全 16 頁)

(21) 出願番号 特願2001-5651 (P2001-5651)

(22) 出願日 平成13年1月12日 (2001.1.12)

(71) 出願人 000202361

総合警備保障株式会社

東京都港区元赤坂1丁目6番6号

(72) 発明者 小川 卯人

東京都港区元赤坂1丁目6番6号 総合警
備保障株式会社内

(74) 代理人 100089118

弁理士 福井 宏明

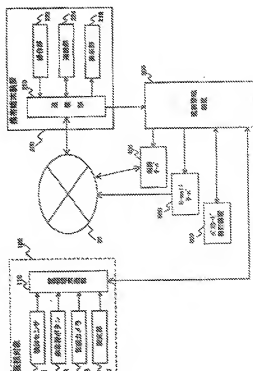
最終頁に続く

(54) 【発明の名称】 監視システム

(57) 【要約】

【課題】 監視領域の画像を画像サーバにアクセスして確認する際に、より強固にプライバシー保護を図った監視システムを提供すること。

【解決手段】 携帯端末装置200が、監視対象100の画像を画像サーバ400にアクセスして確認しようとする際のパパスワード認証またはURL入力において、監視管理装置300が、画像サーバ400において管理される所定のアドレスの画像ページを、監視対象100の最新の画像の画像ページに更新するとともに、上記画像ページにアクセスするためのユーザ認証に必要なパスワードまたは画像ページ特定時に必要なURLを発行して携帯端末装置200に返信する。



【特許請求の範囲】

【請求項1】 監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、

前記携帯端末装置は、操作に応じてパスワード要求信号を送信し、前記携帯端末装置からのパスワード要求信号を受信すると、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを取得して前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像サーバ装置にアクセスして画像ページを表示する際に必要なパスワードを発行し、発行したパスワードを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする監視システム。

【請求項2】 監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、

前記監視端末装置は、監視領域内で異常が発生したときに監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信し、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを受信すると、当該受信信号に基づいて前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像サーバ装置にアクセスして画像ページを表示する際に必要なパスワードを発行し、発行したパスワードを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする監視システム。

【請求項3】 前記監視管理装置は、発行したパスワードを前記携帯端末装置に電子メールにより送信することを特徴とする請求項1または2のいずれか1項に記載の監視システム。

【請求項4】 監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監

視システムにおいて、前記携帯端末装置は、操作に応じてURL要求信号を送信し、前記携帯端末装置からのURL要求信号を受信すると、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを取得して前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像ページを特定する際に必要なアドレスとなるURL (Uniform Resource Locator) を発行し、発行したURLを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする監視システム。

【請求項5】 監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、前記監視端末装置は、監視領域内で異常が発生したときに監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信し、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを受信すると、当該受信信号に基づいて前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像ページを特定する際に必要なアドレスとなるURLを発行し、発行したURLを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする監視システム。

【請求項6】 前記監視管理装置は、発行したURLを前記携帯端末装置に電子メールにより送信することを特徴とする請求項4または5のいずれか1項に記載の監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、異常検知センサ、非常押ボタンおよび監視カメラ等が設置された建物等の監視対象領域において、異常検知センサにより異常事態が検知された際や非常押ボタンが操作された際、またはユーザが要求した際に、監視カメラによって撮影された画像や異常の内容等をユーザが携帯する携帯端末装置上で確認できる監視システムに関するものである。

【0002】

【従来の技術】 従来より、建物等の監視対象に、不法侵入、火災、ガス漏れ等を検知する異常検知センサを設置し、異常検知センサが上記各種異常事態の発生を検知した際に、その監視対象の住人等が携帯端末上でその通報を受けることができる監視システムが知られている。こ

に対する回避方法（警備会社への出勤要請等）を任意に決定するようにしている。

【0003】また、上記監視システムにおいて、住人等が携帯端末上で監視対象の警備状態（警備中であるか警備解除中であるか）や保安状態（窓や扉の開閉状態、異常状態の有無、盗警報装置の故障の有無等）を文字や記号あるいは図により表示し、監視対象の状況を確認することができるとしている。

【0004】さらに、上記監視システムにおいて、監視対象に監視カメラを設け、上記異常検知センサが異常検知した際に、監視カメラによって撮影された画像を携帯端末上に表示可能にすること、通報を受けた者が監視対象の状況を確認することができ、これによりより適切な処置方法の判断をおこなうことができるようにした監視システムが知られている。

【0005】特に、監視区域の警備状態や保安状態あるいは画像の表示を可能とした監視システムでは、監視対象領域内の様子を確認する際、意図の第三者による監視対象領域内の覗き見防止やプライバシー保護等の理由から、画像を見るためにパスワードの入力を条件としている。監視システムにおいて、このようなパスワード入力による表示は、例えば、特開2000-40196号、特開2000-36088号、特開平10-40485号に開示されている。

【0006】

【発明が解決しようとする課題】しかしながら、上記従来の監視システムでは、パスワードが固定であるため、一度第三者にパスワードが盗まれてしまうと、その後はその第三者が常に監視対象領域内の様子を見ることができてしまうという問題があった。

【0007】また、このような問題を解決するため、定期的に暗証番号を変更する等の対策も考えられるが、この作業を住人等の本監視システムの利用者が定期的におこなうには手間がかかるという問題がある。

【0008】本発明は、上記課題を解決するためになされたものであり、監視対象の関係者が保持する端末装置上にて監視対象領域での異常の発生を監視することができ、監視システムにおいて、監視区域の警備状態や保安状態および画像を確認するためのパスワードやURL（Uniform Resource Locator）を必要に応じて自動的に変更することで、安全性の向上とプライバシー保護を図った監視システムを提供することを目的とする。

【0009】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1にかかる監視システムにおいては、監視区域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受

つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、前記携帯端末装置は、操作に応じてパスワード要求信号を送信し、前記携帯端末装置からのパスワード要求信号を受信すると、前記監視端末装置から監視区域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを取得して前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像サーバ装置にアクセスして画像ページを表示する際に必要なパスワードを発行し、発行したパスワードを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする。

【0010】この発明によれば、携帯端末装置が、監視区域の画像を画像サーバ装置にアクセスして確認しようとする際、監視管理装置に対して、パスワードの発行を要求し、監視管理装置が、この要求に対して、画像サーバ装置において管理される所定のアドレスの画像ページを、監視区域の最新の画像の画像ページに更新するとともに、上記画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して携帯端末装置に送信するので、ユーザは、必要に応じてそのパスワードを用いて監視区域の画像を確認することができる。

【0011】また、請求項2にかかる監視システムにおいては、監視区域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの送信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、前記監視端末装置は、監視区域内で異常が発生したときに監視区域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信し、前記監視端末装置から監視区域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを受信すると、当該受信信号に基づいて前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像サーバ装置にアクセスして画像ページを表示する際に必要なパスワードを発行し、発行したパスワードを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする。

【0012】この発明によれば、監視区域において異常が発生した場合に監視端末装置から監視管理装置に対して各種情報や画像が送信された際に、監視管理装置が、画像サーバ装置において管理される所定のURLの画像ページを更新するとともに、上記画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して携帯端末装置に送信するので、ユーザは、監視区域の異常

の画像を確認することができる。

【0013】また、請求項3にかかる監視システムにおいては、請求項1または請求項2のいずれか1項に記載の発明において、前記監視管理装置は、発行したパスワードを前記携帯端末装置に電子メールにより送信することを特徴とする。

【0014】この発明によれば、監視管理装置が、画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して、そのパスワードを電子メールにより携帯端末装置に送信するので、ユーザは、電子メールによりパスワードを取得して、そのパスワードを用いて監視領域の画像を確認することができる。

【0015】また、請求項4にかかる監視システムにおいては、監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置と、前記画像サーバ装置にアクセスして画像ページを表示する携帯端末装置と、を具備して構成される監視システムにおいて、前記携帯端末装置は、操作に応じてURL要求信号を送信し、前記監視端末装置からのURL要求信号を受信すると、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを取得して前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像ページを特定する際に必要なアドレスとなるURL (Uniform Resource Locator) を発行し、発行したURLを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする。

【0016】この発明によれば、携帯端末装置が、監視領域の画像を画像サーバ装置にアクセスして確認しようとする際のURL入力において、まず、監視管理装置に対して、URLの発行を要求し、監視管理装置は、この要求に対して、画像サーバ装置において管理される所定のURLの画像ページを、監視領域の最新の画像の画像ページに更新するとともに、上記画像ページを特定するためのURLを発行し、発行したURLによって上記画像ページが特定されるようにURLを変更した後、上記URLを携帯端末装置に送信するので、ユーザは、そのURLを用いて監視領域の画像を確認することができる。

【0017】また、請求項5にかかる監視システムにおいては、監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信する監視端末装置と、監視端末装置からの受信信号に基づいて文字、記号、図、画像の少なくとも1つにより作成される画像ページを管理する画像サーバ装置

を示す携帯端末装置と、を具備して構成される監視システムにおいて、前記監視端末装置は、監視領域内で異常が発生したときに監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを送信し、前記監視端末装置から監視領域の警備状態に関する情報、保安状態に関する情報、監視区域内を撮影した画像の少なくとも1つを受信すると、当該受信信号に基づいて前記画像サーバの画像ページを更新するとともに、前記携帯端末装置が前記画像ページを特定する際に必要なアドレスとなるURLを発行し、発行したURLを前記携帯端末装置に送信する監視管理装置を備えたことを特徴とする。

【0018】この発明によれば、監視領域において異常が発生した場合に監視端末装置から監視管理装置に対して各種情報や画像が送信された際に、監視管理装置が、画像サーバ装置において管理される所定のURLの画像ページを更新するとともに、上記画像ページを特定するためのURLを発行し、発行したURLによって上記画像ページが特定されるようにURLを変更した後、上記URLを携帯端末装置に送信するので、ユーザは、そのURLを用いて監視領域の画像を確認することができる。

【0019】また、請求項6にかかる監視システムにおいては、請求項4または5のいずれか1項に記載の発明において、前記監視管理装置は、発行したURLを前記携帯端末装置に電子メールにより送信することを特徴とする。

【0020】この発明によれば、監視管理装置が、画像ページにアクセスするために必要なURLを発行して、そのURLを電子メールにより携帯端末装置に送信するので、ユーザは、電子メールによりURLを取得して、そのURLを用いて監視領域の画像を確認することができる。

【0021】

【発明の実施の形態】以下に、本発明にかかる監視システムの実施の形態を図面に基いて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【0022】(実施の形態1) 図1は、実施の形態1にかかる監視システムについて説明する。実施の形態1にかかる監視システムは、ユーザが携帯する携帯端末装置からの要請により、画像サーバに管理されている監視対象の画像を見るためのパスワードを発行し、発行したパスワードを予め決められた携帯端末装置にメールで通知することを特徴としている。

【0023】図1は、実施の形態1にかかる監視システムの概略構成を示すブロック図である。図1に示す監視システムは、建物全体、ビルの一室、個人宅等の監視したい一定の領域である監視対象100と、監視対象100

等)が所有する携帯端末装置200と、携帯端末装置200からの画像配信要求を受け付けるとともに、監視対象100の最新の画像を取得し、パスワードを発行する監視管理装置300と、を備えて構成される。

【0024】また、実施の形態1にかかる監視システムは、監視対象の画像を保持して管理するとともに、その画像をWebページとして提供する画像サーバ400と、携帯端末装置200との電子メール(以下、E-mailと称する。)の送受信を管理制御するE-mailサーバ500と、パスワードを発行するパスワード発行装置600と、を備え、これら画像サーバ400、E-mailサーバ500およびパスワード発行装置600は、上記監視管理装置300に接続されている。また、携帯端末装置200、画像サーバ400およびE-mailサーバ500は、インターネット80にも接続されている。

【0025】図1に示すように、監視対象100には、検知センサ121、非常押ボタン123、監視カメラ125、設定部127および監視端末装置110が設置される。ここで、検知センサ121は、火災による煙を感知する煙感知器、火災による熱を感知する熱感知器、侵入者を検知するためのマグネットセンサや赤外線検知センサ等の種々のセンサであり、火災や侵入者などの異常事態を検知した際に異常検知信号を出力する。

【0026】また、非常押ボタン123は、監視対象100において急病人が発生した場合や監視対象100に強盗が押し入るなどの異常事態発生を通知するために設けられ、操作されると異常検知信号を出力する。監視カメラ125は、監視対象100の異常事態発生時における状況を撮影するために設けられ、監視対象100を撮像して画像データを出力する。

【0027】設定部127は、カードや暗証番号を利用した操作によって、監視端末装置110の監視状態と監視解除状態を設定するための手段であり、通常、監視対象100に人がいる場合は監視解除状態に設定され、不在となる場合は監視状態に設定される。

【0028】監視端末装置110は、専用回線や公共回線を介して監視管理装置300と接続されており、上記した監視カメラ125からの画像データを監視管理装置300に送信する。なお、この監視端末装置110は、検知センサ121や非常押ボタン123によって異常が検知された際に、その通報を携帯端末装置200に発することもある。

【0029】また、図1に示すように、携帯端末装置200は、通話部210、操作部222、通信部224および表示部226を備えて構成され、ここでは携帯電話を想定している。ここで、通信部210は、インターネット80を介して画像サーバ400やE-mailサーバ500と通信し、また無線回線やその他の公共回線を介

スである。操作部222は、ユーザによってダイヤルやその他の応答操作、または携帯端末装置200に付属している種々の機能を発動させるための複数のボタンやスイッチであり、特に、画像を表示するための各種操作(画像表示/非表示、スクロール、画像の切換えなど)をおこなうための手段である。通信部224は、通常の電話による通話をとおこなうためのスピーカやマイクである。そして、表示部226は、画像サーバ400にアクセスして取得した画像データを表示する液晶ディスプレイ等の表示手段である。

【0030】以下に、実施の形態1にかかる監視システムの動作について説明する。図2は、実施の形態1にかかる監視システムの動作を示すフローチャートである。まず、監視対象100の関係者(住人等)であるユーザが携帯端末装置200を用いて、監視管理装置300へとパスワードの発行を要求するパスワード発行要求信号を送信する(ステップS101)。このパスワード発行要求信号には、少なくとも当該携帯端末装置200を識別するための端末コードが含まれている。なお、携帯端末装置200と監視管理装置300との間の通信は、特に限定しないが、例えば無線回線を介しておこなう。

【0031】監視管理装置300は、監視端末装置110に対応する携帯端末装置200の端末コードとURL(Uniform Resource Locator)を予め記憶しており、携帯端末装置200からパスワード発行要求信号を受けると、当該パスワード発行要求信号に含まれる端末コードに対応する監視端末装置110から、監視カメラ125によって撮影された最新の画像を取得する(ステップS201)。なお、監視管理装置300と監視端末装置110との間の通信は、特に限定しないが、例えば公共の電話回線を介しておこなう。

【0032】つづいて、監視管理装置300は、取得した画像から画像ページを作成し(ステップS202)、画像サーバ400に対し、当該監視端末装置110のURLで特定されるWeb用の画像ページを、新たに作成した画像ページに更新することを要求する画像ページ更新要求信号を送信する(ステップS203)。なお、この画像ページ更新要求信号には、新たに作成した画像ページの情報も含まれている。画像サーバ400は、監視管理装置300から画像ページ更新要求信号を受けると、上記所定のURLで特定される画像ページを、新たに作成された画像ページに更新する(ステップS301)。

【0033】一方で、監視管理装置300は、パスワード発行装置600に対し、パスワードの発行を要求するパスワード発行要求信号を送信する(ステップS204)。パスワード発行装置600は、監視管理装置300からパスワード発行要求信号を受けると、任意のパス

たパスワードを監視管理装置300に送信する(ステップS402)。

【0034】監視管理装置300は、パスワード発行装置600からパスワードを受けると、画像サーバ400に、上記監視端末装置100の画像ページを見るためのパスワードを新たに発行されたパスワードに変更するためのパスワード変更要求信号を送信する。画像サーバ400は、監視管理装置300からパスワード変更要求信号を受けると、上記監視端末装置100の画像ページを見るためのパスワードを上記パスワード変更要求信号に含

10

まれた新たなパスワードに変更する。
【0035】また、監視管理装置300は、パスワード発行装置600からパスワードを受けると、そのパスワードを記載したE-mailを上記携帯端末装置200宛に送信する。このE-mailの送信は、実際には、監視管理装置300がE-mailサーバ500に対してE-mail送信要求を依頼し(ステップS205)、E-mailサーバ500によって携帯端末装置200へと配信される(ステップS301)。

【0036】ユーザは、携帯端末装置200において、上記E-mailの受信を確認すると、所定のWebページのURL。この場合、監視対象100の画像を確認することができる画像ページのURLを入力することで(ステップS102)、その画像ページを管理している画像サーバ400へと、上記画像ページの配信を要求する画像ページ配信要求信号を送信する(ステップS103)。

20

【0037】画像サーバ400は、携帯端末装置200から、画像ページ配信要求信号を受けると、そのユーザが画像ページを取得するのに適正であるかどうかの認証をおこなうために、パスワード入力画面を送信する(ステップS302)。携帯端末装置200が、画像サーバ400からパスワード入力画面を取得すると、ユーザは、そのパスワード入力画面の入力フォームに従ってパスワードを入力する(ステップS104)。特に、このパスワードは、上記ステップS501において送信されたE-mailに記載されたパスワードである。

30

【0038】携帯端末装置200は、入力されたパスワードを画像サーバ400へと送信し(ステップS106)、画像サーバ400は、このパスワードが正当なものであるかどうかを照合する(ステップS303)。このパスワードの照合は、パスワード入力画面に定義づけられたCGI(Common Gate Interface)等のプログラムによっておこなわれ、特に、上記ステップS401においてパスワード発行装置が発行したパスワードを照合対象としている。

【0039】画像サーバ400は、上記パスワードが正当なものであると判断すると、上記ステップS301において更新した画像ページを携帯端末装置200に送信

の画像ページを表示する(ステップS106)。これにより、ユーザは監視対象100の状況を確認することができる。

【0040】なお、セキュリティ性を向上させるため、画像サーバ400は、携帯端末装置200が画像ページを受信した後に、ユーザによって画像確認の通知が送信された際、または画像ページを更新してから一定時間経過した際に、その画像ページの画像を削除するようにしてもよい。また、携帯端末装置200が同じ画像の画像ページを一定の回数受信した際に、その画像ページを消去してもよい。さらに、一度、ユーザ端末200から正当なアクセスがあった場合には、そのパスワードを無効にすることで、よりセキュリティの向上を図ることができる。

【0041】以上に説明したとおり、実施の形態1にかかる監視システムによれば、携帯端末装置200が、監視対象100の画像を画像サーバにアクセスして確認しようとする際のパスワード認証において、まず、監視管理装置300に対して、パスワードの発行を要求し、監視管理装置300は、この要求に対して、画像サーバ400が管理する所定のURLの画像ページを、監視対象100の最新の画像の画像ページに更新するとともに、パスワード発行装置600から、上記画像ページにアクセスするために必要なパスワードを取得して、そのパスワードをE-mailにより携帯端末装置200へと送信し、ユーザは、E-mailによりパスワードを取得して、そのパスワードを用いて監視対象100の画像を確認することができるので、画像ページにアクセスするためのパスワードを盗用されても、そのパスワードを用いた画像ページの確認は一時的なものとなり、プライバシーが継続的に置かれてしまうことを防止することができる。

【0042】(実施の形態2) つぎに、実施の形態2にかかる監視システムについて説明する。実施の形態2にかかる監視システムは、監視対象の携帯端末装置における異常検知をトリガーにして、画像サーバに管理されている監視対象の画像を見るためのパスワードを発行し、発行したパスワードを予め決められた携帯端末装置にメールで通知することを特徴としている。

【0043】実施の形態2にかかる監視システムの構成は、図1と同様であるのでここではその説明を省略する。但し、監視端末装置100は、上記した検知センサ121から異常検知信号が出力されたとき、または上記した非常押ボタン123から異常報道信号が出力されたときに、監視管理装置300に対して異常事態発生を知らせるための通報とともに上記した監視カメラ125で撮像された異常発生時の画像を送信する。

【0044】以下に、実施の形態2にかかる監視システムの動作について説明する。図3は、実施の形態2にか

40

まず、監視対象100に設置された監視端末装置110が、検知センサ121や非常押ボタン123によって異常を検知すると(ステップS601)、監視端末装置110は、少なくとも異常を検知したときに監視カメラ125から入力している画像データを監視管理装置300に送信する(ステップS602)。そして、監視管理装置300は、実施の形態1において説明したように、取得した画像データから画像ページを作成する(ステップS202)。

【0045】 つづいて監視管理装置300、画像サーバ400、パスワード発行装置600および携帯端末装置200の処理は、実施の形態1と同様であるので、ここでは、図3において、図2と共通する処理について同一符号を付し、それらの説明を省略する。但し、ステップS501において携帯端末装置200に送信されるE-mailには、パスワードのみならず、異常事態が生じた旨のメッセージを記載する。特に、どのような種類の検知センサによる異常検知なのかといった通知の種類をそのメッセージに含めることで、ユーザが画像を確認する際に、画像のどの場所を注目すればよいかわかり、状況確認の見落としを防ぐことができる。

【0046】 なお、実施の形態2においては、携帯端末装置200へのパスワードの通知とともに異常事態の発生を通知をおこなっているため、特に携帯端末装置200が携帯電話であって通信不可域に位置する場合には、監視対象100の異常事態に対する処置が遅れてしまう。そこで、そのような処置の遅れを防ぐため、E-mailサーバ500は、携帯端末装置200にE-mailを送信後、一定時間しても受信確認ができない場合、他の予め登録された関係者宛にE-mailを送信するようにしてもよい。

【0047】 なお、この場合、先に送信したユーザとその宛に送信した他の関係者とが、ともに警備会社等に通報をおこなうなどの二重の処置が施されてしまうのを防ぐため、すでにE-mailを送信しているユーザに対しては、他の関係者にE-mailを送信したことや異常状態の処置結果(警備会社への出動要請の有無等)を通知するようにしてもよい。

【0048】 以上に説明したとおり、実施の形態2にかかる監視システムによれば、監視対象100に設置された監視端末装置110から監視管理装置300に対して異常事態の通報があった際に、監視管理装置300が、画像サーバ400により管理される所定のURLの画像ページに、監視対象100の最新の画像の画像ページに更新するとともに、パスワード発行装置600から、上記画像ページにアクセスするために必要なパスワードを取得して、そのパスワードと異常事態の通報とをE-mailにより携帯端末装置200へと送信し、ユーザは、そのE-mailにより取得したパスワードを用い

監視対象100に異常が発生した旨を知得することができるとともに、監視対象100の画像ページにアクセスするためのパスワードを盗用されても、そのパスワードを用いた画像ページの確認は一時的なものとなり、プライバシーが継続的に置かれてしまうことを防止することができる。

【0049】 (実施の形態3) つづいて、実施の形態3にかかる監視システムについて説明する。実施の形態3にかかる監視システムは、ユーザが携帯する携帯端末装置からの要請により、画像サーバに管理されている監視対象の画像ページにアクセスするためのURLを発行し、発行したURLを予め決められた携帯端末装置にメールで通知することを特徴としている。

【0050】 実施の形態3にかかる監視システムの構成は、図1と同様であるのでここではその説明を省略する。但し、パスワード発行装置600は、URL発行装置600に置換する。

【0051】 以下に、実施の形態3にかかる監視システムの動作について説明する。図4は、実施の形態3にかかる監視システムの動作を示すフローチャートである。まず、監視対象100の関係者(社人等)であるユーザが携帯端末装置200を用いて、監視管理装置300へとURLの発行を要求するURL発行要求信号を送信する(ステップS111)。このURL発行要求信号には、少なくとも当該携帯端末装置200を識別するための端末コードが含まれている。

【0052】 監視管理装置300は、携帯端末装置200からURL発行要求信号を受けると、当該URL発行要求信号に含まれる端末コードに対応する監視端末装置110から、監視カメラ125によって撮影された最新の画像を取得する(ステップS211)。

【0053】 つづいて、監視管理装置300は、取得した画像から画像ページを作成し(ステップS212)、画像サーバ400に対し、当該監視端末装置110のURLで特定されるWeb上の画像ページを、新たに作成した画像ページに更新することを要求する画像ページ更新要求信号を送信する(ステップS213)。なお、この画像ページ更新要求信号には、新たに作成した画像ページの情報も含まれている。画像サーバ400は、監視管理装置300から画像ページ更新要求信号を受けると、上記特定のURLで特定される画像ページを、新たに作成された画像ページに更新する(ステップS311)。

【0054】 一方で、監視管理装置300は、URL発行装置600に対し、URLの発行を要求するURL発行要求信号を送信する(ステップS214)。URL発行装置600は、監視管理装置300からURL発行要求信号を受けると、URLを生成して発行し(ステップS411)、発行したURLを監視管理装置300に送

【0055】監視管理装置300は、URL発行装置600からURLを受けると、画像サーバ400に、上記所定のURLを新たに発行されたURLに変更するためのURL変更要求信号を送信する(ステップS215)。画像サーバ400は、監視管理装置300からURL変更要求信号を受けると、上記所定のURL、すなわち監視対象100の画像を表示するための画像ページを特定するURLを、上記URL変更要求信号に含まれる新たなURLに変更する(ステップS212)。

【0056】また、監視管理装置300は、上記新たなURLを記載したE-mailを上記携帯端末装置200宛に送信する。このE-mailの送信は、実際には、監視管理装置300がE-mailサーバ500に対してE-mail送信要求を依頼し(ステップS216)、E-mailサーバ500によって携帯端末装置200へ配信される(ステップS611)。

【0057】ユーザは、携帯端末装置200において、上記E-mailの受信を確認すると、そのE-mailに新たなURLとして記載されたURLを入力することで(ステップS112)、画像サーバ400に対し、そのURLで特定される画像ページの配信を要求する画像ページ配信要求信号を送信する(ステップS113)。

【0058】画像サーバ400は、携帯端末装置200から、画像ページ配信要求信号を受けると、上記ステップS311において更新した画像ページを携帯端末装置200に送信する(ステップS313)。携帯端末装置200は、この画像ページを受信する(ステップS114)。これにより、ユーザは監視対象100の状況を確認することができる。

【0059】なお、セキュリティ性を向上させるため、画像サーバ400は、携帯端末装置200が画像ページを受信した後に、ユーザによって画像確認の通知が送信された際、または画像ページを更新してから一定時間経過した際に、その画像ページの画像を消去するようにしてもよい。また、携帯端末装置200が同じ画像の画像ページを一定の回数受信した際に、その画像ページを消去してもよい。

【0060】以上に説明したとおり、実施の形態3にかかる監視システムによれば、携帯端末装置200が、監視対象100の画像を画像サーバにアクセスして確認しようとするURL入力において、まず、監視管理装置300に対して、URLの発行を要求し、監視管理装置300は、この要求に対して、画像サーバ400が管理する所定のURLの画像ページを、監視対象100の最新の画像の画像ページに更新するとともに、URL発行装置600から、上記画像ページを特定するURLを取得し、そのURLによって上記画像ページが特定されるようにURLを変更した後、そのURLをE-mail

mailにより新しいURLを取得して、そのURLを用いて監視対象100の画像を確認することができるので、画像ページにアクセスするためのURLが知られても、そのURLによってアクセスされる画像ページの確認は一時的なものとなり、プライバシーが継続的に習せられてしまうことを防止することができる。

【0061】(実施の形態4) つぎに、実施の形態4にかかる監視システムについて説明する。実施の形態4にかかる監視システムは、監視対象の監視端末装置における異常検知をトリガーにして、画像サーバに管理されている監視対象の画像を見るためのURLを発行し、発行したURLを予め決められた携帯端末装置にメールで通知することを特徴としている。

【0062】実施の形態4にかかる監視システムの構成は、図1と同様であるのでここではその説明を省略する。但し、監視端末装置110は、上記した検知センサ121から異常検知信号が出力されたとき、または上記した非常ボタン123から異常検知信号が出力されたときに、監視管理装置300に対して異常事態発生を知らせるための通報とともに上記した監視カメラ125で撮像された異常発生時の画像を送信する。また、パスワード発行装置600は、URL発行装置600に接続する。

【0063】以下に、実施の形態4にかかる監視システムの動作について説明する。図5は、実施の形態4にかかる監視システムの動作を示すフローチャートである。まず、監視対象100に設置された監視端末装置110が、検知センサ121や非常ボタン123によって異常を検知すると(ステップS601)、監視端末装置110は、少なくとも異常を検知したときに監視カメラ125から入力している画像データを監視管理装置300に送信する(ステップS602)。そして、監視管理装置300は、実施の形態3において説明したように、取得した画像データから画像ページを作成する(ステップS212)。

【0064】つづき監視管理装置300、画像サーバ400、URL発行装置600および携帯端末装置200の処理は、実施の形態3と同様であるので、ここでは、図3において、図2と共通する処理について同一符号を付し、それらの説明を省略する。但し、ステップS511において携帯端末装置200に送信されるE-mailには、新しいURLのみならず、異常事態が生じた旨のメッセージを記載する。特に、どのような種類の検知センサによる異常検知なのかといった通報の種類をそのメッセージに含めることで、ユーザが画像を確認する際に、画像のどの場所を注目すればよいかかわかり、状況確認の見落としを防ぐことができる。

【0065】なお、実施の形態4においては、携帯端末装置200への新たなURLの通知とともに異常事態

200が携帯電話であって通信不可能な圏外に位置する場合に、監視対象100の異常事態に対する処置が遅れてしまうが、その場合の対処方法は、実施の形態2において説明したとおりである。

【0066】以上に説明したとおり、実施の形態4にかかる監視システムによれば、監視対象100に設置された監視端末装置110から監視管理装置300に対して異常事態の通報があった際に、監視管理装置300が、画像サーバ400により管理される所定のURLの画像ページを、監視対象100の最新の画像の画像ページに更新するとともに、URL発行装置600から、上記画像ページにアクセスするために必要な新たなURLを取得して、そのURLによって上記画像ページが特定されるようにURLを変更した後、新たなURLと異常事態の通報とをE-mailにより携帯端末装置200へと送信し、ユーザは、そのE-mailによりURLを取得して、新たなURLを用いて監視対象100の画像を確認することができるので、監視対象100に異常が発生した旨を知得することができる。また、監視対象100の画像ページにアクセスするためのURLを盗用されても、そのURLを用いた画像ページの確認は一時的なものとなり、プライバシーが継続的に冒されてしまうことを防止することができる。

【0067】以上に説明した実施の形態1〜4においては、監視システムの構成を、図1に示すように、携帯端末装置200および監視端末装置110と監視管理装置300との間がインターネットを経由しない通信経路によって接続され、画像サーバ400およびE-mailサーバ500が直接に監視管理装置300に接続される点に在り、これらの接続をインターネットを経由しておこなうこともできる。

【0068】例えば、図6に示すように、監視管理装置300と監視端末装置110をインターネットに接続可能な構成とし、携帯端末装置200から監視管理装置300へのパスワード発行要求またはURL発行要求と、監視端末装置110から監視管理装置300への通報や画像データの送信とをインターネット80を介しておこなうこともできる。この場合、監視管理装置300と画像サーバ400およびE-mailサーバ500との間の通信もインターネット80を介しておこなうことができる。

【0069】また、実施の形態1〜4においては、図1に示すように、監視管理装置300と監視端末装置110とは別装置であるとしたが、図7に示すように、監視管理装置300の機能を監視端末装置110上で実現し、監視端末装置110が、パスワード発行装置（またはURL発行装置）600と直接に通信をおこなうこともよい。よって、この場合、画像ページの作成は、監視端末装置110がこなうことになる。

監視装置300とパスワード発行装置（またはURL発行装置）600とを別装置としたが、パスワード発行装置（またはURL発行装置）600の機能を監視管理装置300上で実現してもよい。

【0071】なお、実施の形態1〜4においては、監視管理装置300は、監視端末装置110から画像データを取得し、この画像データに基づいて画像ページを作成し画像サーバに送信するようにしているが、監視区域の警備状態（警備中であるか警備解除中であるか）や保安状態（窓や扉の開閉状態、異常状態の有無、設備機器の故障等）に関する情報を取得し、これらの情報をもとに画像ページを作成するようにしてもよい。この場合、これらの情報は文字や記号あるいは図により表示される。

【0072】また、実施の形態1および2に記載した監視システムでは、パスワードのみを変更するようにしており、実施の形態3および4に記載した監視システムでは、URLのみを変更するようにしているが、両者を組み合わせることで、より安全性を向上させることができる。

【0073】ただし、住人等が上記携帯端末装置200を紛失し、悪意の第三者にこの携帯端末装置200がわたってしまった場合、この携帯端末装置200を用いて第三者が監視領域の画像ページをいつでも盗み見ることでできてしまうという問題がある。そこで、上記実施の形態1〜4において、上記携帯端末装置200は、住人等の正規の所有者により予め決められているパスワードが操作部210から入力した場合にのみパスワードあるいはURLの発行要求や画像ページの配信要求をおこなうことができるようにしてよい。これにより、さらに安全性を向上させることができる。

【0074】

【発明の効果】以上に、説明したとおり、請求項1の発明によれば、携帯端末装置が、監視領域の画像を画像サーバ装置にアクセスして確認しようとする際、監視管理装置に対して、パスワードの発行を要求し、監視管理装置が、この要求に対して、画像サーバ装置において管理される所定のアドレスの画像ページを、監視領域の最新の画像の画像ページに更新するとともに、上記画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して携帯端末装置に送信するので、ユーザは、必要に応じてそのパスワードを用いて監視領域の画像を確認することができ、画像ページにアクセスするためのパスワードを盗用されても、そのパスワードを用いた画像ページの確認は一時的なものとなり、悪意の第三者による画像ページの継続的な盗み見を防止することが可能になるという効果を奏する。

【0075】また、請求項2の発明によれば、監視領域において異常が発生した場合に監視端末装置から監視管理装置に対して各種情報や画像が送信された際に、監視

URLの画像ページを更新するとともに、上記画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して携帯端末装置に送信するので、ユーザは、監視領域の異常事態の知得とともに、そのパスワードを用いて監視領域の画像を確認することができ、画像ページにアクセスするためのパスワードを盗用されても、そのパスワードを用いた画像ページの確認は一時的なものとなり、悪意の第三者による画像ページの継続的な盗み見を防止することが可能になるという効果を奏する。

【0076】また、請求項8の発明によれば、監視管理装置が、画像ページにアクセスするためのユーザ認証に必要なパスワードを発行して、そのパスワードを電子メールにより携帯端末装置に送信するので、ユーザは、電子メールによりパスワードを取得して、そのパスワードを用いて監視領域の画像を確認することができ、既存の電子メールシステムを利用して安価に監視システムを構築することが可能になるという効果を奏する。

【0077】また、請求項9の発明によれば、携帯端末装置が、監視領域の画像を画像サーバ装置にアクセスして確認しようとする際のURL入力において、まず、監視管理装置に対して、URLの発行を要求し、監視管理装置は、この要求に対して、画像サーバ装置において管理される所定のURLの画像ページを、監視領域の最新の画像の画像ページに更新するとともに、上記画像ページを特定するためのURLを発行し、発行したURLによって上記画像ページが特定されるようにURLを変更した後、上記URLを携帯端末装置に送信するので、ユーザは、そのURLを用いて監視領域の画像を確認することができ、画像ページにアクセスするためのURLが知られても、そのURLによってアクセスされる画像ページの確認は一時的なものとなり、悪意の第三者による画像ページの継続的な盗み見を防止することが可能になるという効果を奏する。

【0078】また、請求項5の発明によれば、監視領域において異常が発生した場合に監視端末装置から監視管理装置に対して各種情報や画像が送信された際に、監視管理装置が、画像サーバ装置において管理される所定のURLの画像ページを更新するとともに、上記画像ページを特定するためのURLを発行し、発行したURLによって上記画像ページが特定されるようにURLを変更した後、上記URLを携帯端末装置に送信するので、ユーザは、そのURLを用いて監視領域の画像を確認することができ、画像ページにアクセスするためのURLが知られても、そのURLによってアクセスされる画像ページ

のURLの確認は一時的なものとなり、悪意の第三者による画像ページの継続的な盗み見を防止することが可能になるという効果を奏する。

【0079】また、請求項6の発明によれば、監視管理装置が、画像ページにアクセスするために必要なURLを発行して、そのURLを電子メールにより携帯端末装置に送信するので、ユーザは、電子メールによりURLを取得して、そのURLを用いて監視領域の画像を確認することができ、既存の電子メールシステムを利用して安価に監視システムを構築することが可能になるという効果を奏する。

【図面の簡単な説明】

【図1】実施の形態1にかかる監視システムの概略構成を示すブロック図である。

【図2】実施の形態1にかかる監視システムの動作を示すフローチャートである。

【図3】実施の形態2にかかる監視システムの動作を示すフローチャートである。

【図4】実施の形態3にかかる監視システムの動作を示すフローチャートである。

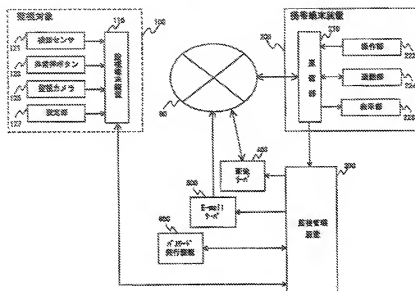
【図5】実施の形態4にかかる監視システムの動作を示すフローチャートである。

【図6】実施の形態1～4にかかる監視システムの他の概略構成を示すブロック図である。

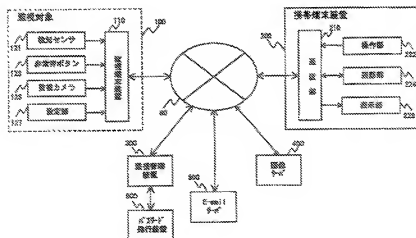
【図7】実施の形態1～4にかかる監視システムの他の概略構成を示すブロック図である。

【符号の説明】

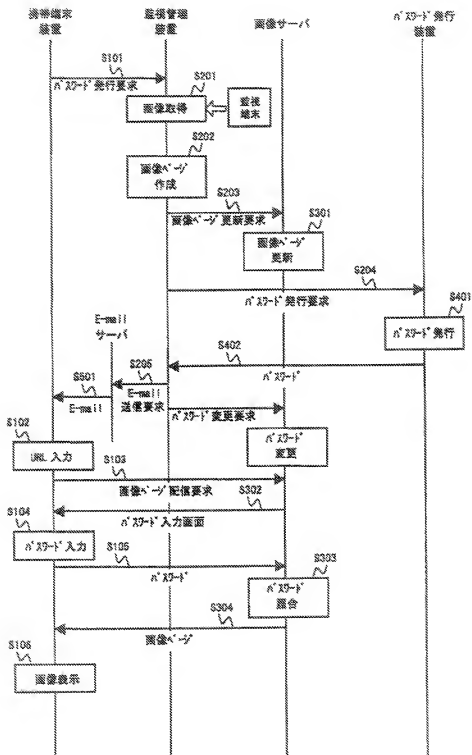
80 インターネット
100 監視対象
110 監視端末装置
121 検知センサ
123 非常押ボタン
125 監視カメラ
127 設定部
200 携帯端末装置
210 通信部
222 操作部
224 送話部
226 表示部
300 監視管理装置
400 画像サーバ
500 E-mailサーバ
600 パスワード発行装置

[illegible]

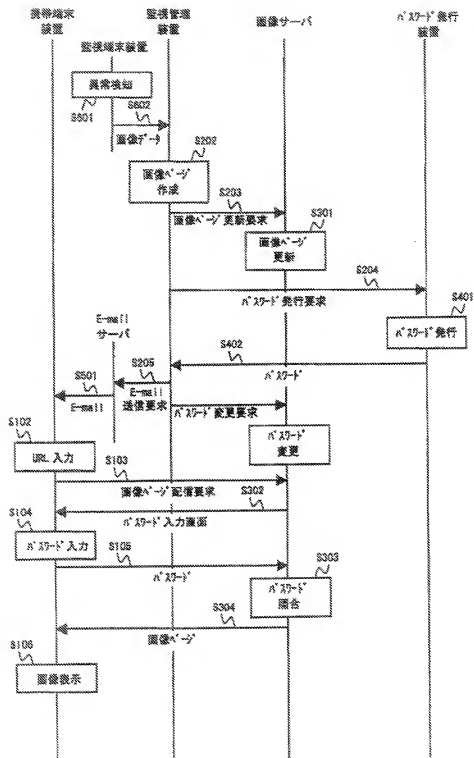
1200



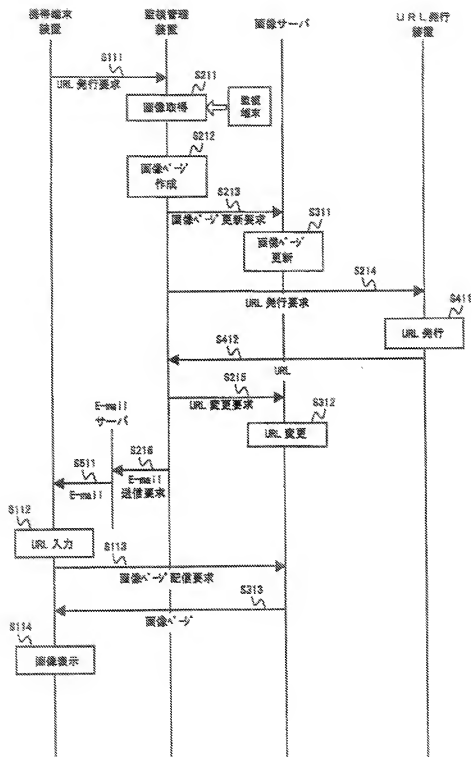
【図2】



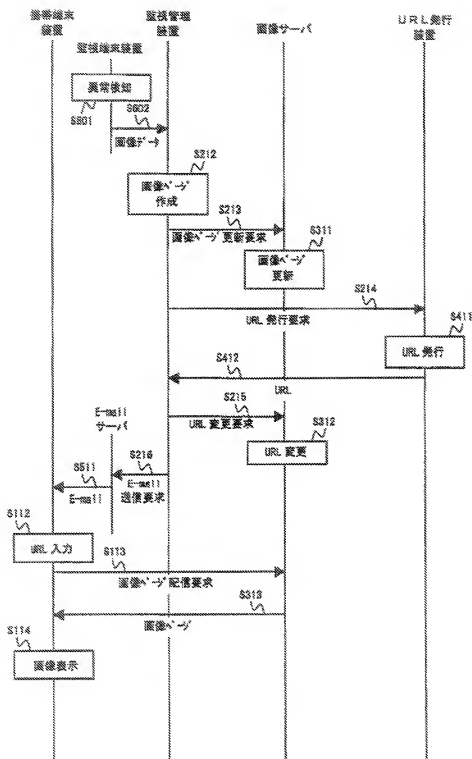
【図3】



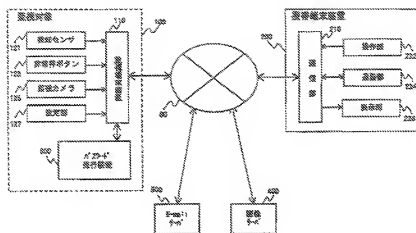
【図4】



【図5】



【図7】



フロントページの続き

Fターム(参考) 5C064 AA01 CA04 CC02 DA09 GB01
 GD08 HA18
 5C064 BA01 BA07 BB02 BC18 BC23
 BD02 BD08 BD09
 5C067 AA02 AA03 AA10 BB21 BB74
 DD04 DD06 EE20 FF01 FF04
 FP23 GG66 GG70 GG83